Out with the Old, In with the New: Examining National Cybersecurity Strategy Changes over Time

W. Alec Cram
University of Waterloo
wacram@uwaterloo.ca

Jonathan Yuan
University of Waterloo
j95yuan@uwaterloo.ca

Abstract

The development and implementation of a national cybersecurity strategy (NCS) is becoming increasingly common for countries around the world that seek to define an approach for addressing their cybersecurity risks. Although past research has sought to classify the individual characteristics contained within an NCS, it remains unclear how the core content within a strategy evolves over time in the face of new cyber threats and fluctuating priorities. By better understanding such changes (and their underlying drivers), policy makers can be increasingly attuned to essential NCS updates and citizens can more readily evaluate the adequacy of their country's plans. This study examines multiple NCS versions in Canada, the United Kingdom, and Australia using a qualitative, content analysis approach. Our results point to four core themes that characterize NCS stability and change over time. Based on our observations, we articulate several theoretical propositions and outline a plan for future research.

1. Introduction

The leaders of countries around the world are becoming increasingly attuned to the growing level of cybersecurity risks facing their nations. The threat of targeted attacks against critical infrastructure and national security apparatus, as well as the specific risks of cybersecurity incidents impacting individual citizens are acknowledged as being extremely high [1].

In response, policy makers in many countries have constructed national cybersecurity strategy (NCS) guidelines [2]. These documents commonly include an articulation of threats, objectives, and plans of action related to cybersecurity events, although no broadly accepted set of norms associated with NCS development has yet been established [3, 4].

Past research highlights the difficulty that policy makers face in defining an NCS that works for government, industry, and civilians [5]. These challenges are particularly acute in developing countries, where economies are emerging and fewer cybersecurity resources are available [3]. Indeed, past research points to notable differences in NCS content across countries [4]. Despite early views that NCS design elements could be relatively uniform around the world, more recent perspectives argue that differences should be expected as a result of factors such as the technical and administrative capabilities of a country [3].

One of the key challenges that policy makers face is the changing environment in which the NCS must apply. This is particularly difficult due to rapid innovation and continually emerging threats [5]. While the first wave of NCS guidelines were released in many countries beginning about a decade ago, those same countries have typically updated and refined their NCS documents in the intervening years to take into account these new realities. However, past research has primarily adopted a cross-sectional, point-in-time assessment of NCS documents, either by comparing the approaches of several countries [e.g., 4, 5, 6] or by conducting an in-depth analysis of a single country [e.g., 7, 8]. Despite the recognition that an NCS should be reviewed and updated every few years [9], there has been little examination of the specific nature of the changes that stem from these updates.

This study seeks to address this opportunity by posing the following research question: *To what extent does the content within a national cybersecurity strategy change (or remain the same) over time?* By better understanding how NCS content evolves from one version to the next, policy makers can be increasingly attuned to the updates that may be necessary to maintain a robust strategy, while citizens can track the continuing refinement of their country's plans over time. Further, insights from our study can benefit research by identifying the underlying factors that drive change (or stability) in NCS documents over time.

To address our research question, we undertook a qualitative, content analysis approach to investigate both initial and revised NCS documents in Canada, the United Kingdom, and Australia. Our findings reveal four core themes that capture elements of both stability and change over time: understanding the current environment; teamwork; security and protective actions; and preparing for the future.

In the next section, we outline the key elements and trends within the study of NCS. We then describe our

URI: https://hdl.handle.net/10125/79617
978-0-9981331-5-7

research methodology and detail the study's results. Next, we discuss how our study advances research and practice in the field. We conclude with directions for future research, including a series of associated theoretical propositions.

2. Conceptual foundations

Broadly, cybersecurity refers to "the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems" [10, p. 41]. In order to achieve these objectives on a national scale, governments are increasingly choosing to design and implement an NCS, which represents a "a national plan of action based upon a national vision to achieve a set of objectives that contribute to the security of the cyberspace domain" [4, p. 4]. In creating an NCS, a country's goal is typically to align government efforts towards cybersecurity improvements [3]. A variety of components can be included in a country's NCS, including articulating a link to other national strategies, highlighting the relevant threats, outlining the nation's vision, objectives and principles for cybersecurity, as well as prescribing detailed plans of action [4].

Three paradigms are attributed to interpreting cybersecurity challenges at a national level, based upon national security theory, economic theory, and public health theory [3, 11]. These paradigms provide a philosophical context for the motivations driving an engagement in an NCS initiative. From a national security perspective, cybersecurity is viewed as a legal issue of importance to the security of the country. Such an approach tends to place importance on the military to influence NCS development. When considering NCS from an economic viewpoint, cybersecurity is perceived as a key element driving commerce. Finally, a public health model of NCS approaches cybersecurity as representing a public good and infers that its effectiveness can have broad benefits to stakeholders [1, 3].

Beyond these philosophical motivations, the practical impetus to develop an NCS tends to originate from three main sources: a desire to protect national security (e.g., protecting state secrets), an interest in jurisprudence (e.g., ensuring adherence to the law), and political interests (e.g., strengthening diplomacy) [5]. However, regardless of the motivation, NCS documents have been criticized in past research for suffering from a lack of common terminology, difficulties in finding a balance between being too strict and too open, and adequately representing the interests of various stakeholders in terms of government, industry, and civilians [4, 5].

Much of the past research on NCS-related topics has examined the characteristics of a particular NCS in place in a few selected countries or regions, such as the USA, the EU, and Japan [12], while other studies consider a wider range of comparisons across ten or more countries [e.g., 13]. Other work has conducted an extensive analysis of a single country, including Israel [14], Myanmar [15], Nigeria [8], and Portugal [7]. Stemming from these studies are guidelines and suggestions on NCS best practices. For example, Newmeyer [3] highlights the importance of having senior political leadership support, establishing a legal framework in order to establish stakeholder responsibilities, and facilitating information campaigns to increase public awareness.

Despite this valuable stream of research, very little attention has been paid to how national cybersecurity strategies change over time. One exception is research by Schallbruch and Skierka [16] who consider three phases of cybersecurity strategy development in Germany during 1991 to 2018. Such longitudinal studies can provide unique insights pertaining to the themes within an NCS that are important and remain so over time, versus those that may only be present in a single NCS version. Over time, as countries develop their strategic direction, important attributes will receive more attention while unimportant attributes will be expected to diminish in importance.

3. Methodology

We utilized a qualitative, content analysis approach to examine the NCS documents in Canada, the United Kingdom, and Australia. Due to our primary focus on identifying elements of change or stability over time, we deemed a qualitative approach to be appropriate in that it would enable an in-depth assessment of the source documents [17, 18]. We also note that past work investigating NCS content commonly draws upon qualitative methods [e.g., 4, 5]. Although the application of longitudinal perspectives is not yet common in the study of NCS documents, past work in other fields has highlighted the importance of considering the factors that drive change in phenomena over time [19, 20].

3.1. Data collection

We used several criteria to determine which countries' NCS documents would be most suitable to study. First, we restricted our focus to countries that had at least two versions of an NCS (i.e., an initial NCS and at least one subsequent revision) that were published in English and publicly available. Second, to make the

NCS changes comparable, we sought countries that had roughly the same interval between NCS versions and were published at roughly the same time (e.g., within two years). Finally, we were interested in obtaining a diverse set of perspectives on NCS approaches and sought to select countries from distinct regions around the world.

We identified three countries that met the inclusion criteria for our study: Canada, the United Kingdom, and Australia. Canada issued its first NCS in 2010 and its second in 2018. In comparison, the United Kingdom issued its first NCS in 2009, as well as revised versions in both 2011 and 2016. Finally, Australia's NCS was first published in 2009, followed by updates in 2016 and again in 2020.

Each NCS was obtained from its country's official federal government website. Due to our study's focus on the NCS, we excluded a review of any supplementary materials (e.g., action plans) from our scope. In total, the combined NCS documents comprised 370 pages of text. Refer to Table 1 for a summary of the NCS documents we assessed.

Table 1. NCS documents listing

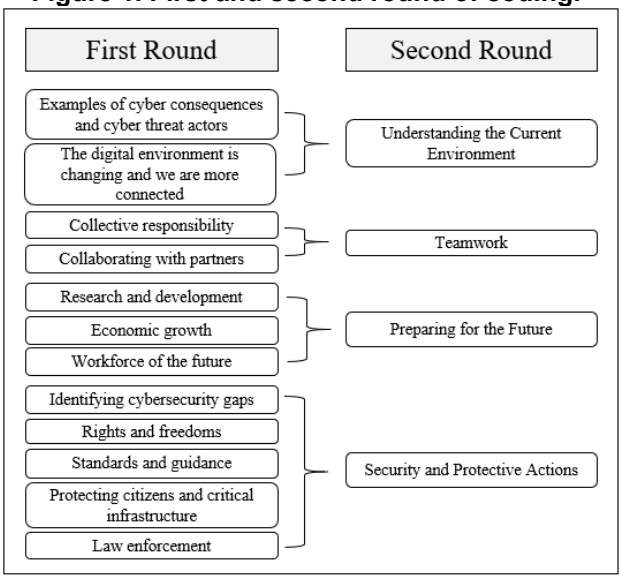
NCS Title	Country	Year	Pages
Canada's Cyber Security Strategy	Canada	2010	17
NCSS: Canada's Vision for Security and Prosperity in the Digital Age	Canada	2018	40
Cyber Security Strategy of the United Kingdom	United Kingdom	2009	32
U.K. Cyber Security Strategy: Protecting and Promoting the U.K. in the Digital World	United Kingdom	2011	43
National Cyber Security Strategy 2016-2021	United Kingdom	2016	80
Cyber Security Strategy	Australia	2009	38
Australia's Cyber Security Strategy	Australia	2016	68
Australia's Cyber Security Strategy 2020	Australia	2020	52

3.2. Data analysis

Our data analysis consisted of qualitative coding of the text passages within each NCS using NVivo software (version 12). We started by examining Canada's NCS documents and carefully reviewed the content with the objective of identifying patterns and themes [21]. As areas of interest were identified within the documents, they were discussed by the author team. This process continued on an iterative basis and these themes were expanded and/or consolidated as new ideas emerged. In NVivo, each theme was initially represented by a first-round code that was linked to a collection of related passages from the NCS. These first-round codes were then consolidated into broader second-round code categories. As the data analysis continued with the NCS documents in the United Kingdom and Australia, we continued to update and refine our coding scheme.

Next, we reviewed the coding patterns that emerged in NVivo for each individual country, with a focus on changes in coding between different versions of the NCS (e.g., Canada 2010 versus Canada 2018). We considered both the quantity, as well as the context of the coded passages, and inferred the relative emphasis and importance of that theme in each NCS document. For example, if the theme "workforce of the future" had two coded passages in Canada's 2010 NCS and ten coded passages in the 2018 NCS, we concluded that relative to the 2010 document, the 2018 version put greater emphasis on the theme's focus. We conducted this within-country analysis for all three countries in our scope. Refer to Figure 1 for details on our first and second round coding activities.

Figure 1. First and second round of coding.



Finally, after comparing the coding results within each country, we moved on to compare our initial observations across the three countries. In particular, we sought to identify if the patterns we had identified in each individual country were similar or different to those patterns from the other countries. In using this approach, we essentially treated each country as a stand-alone case study, with data "snapshots" at each point in time where an NCS was published. In doing so, we

extended the within-case analysis explained above (e.g., how the content in Canada's NCS changed over time) to engage in a cross-case analysis (e.g., how the changes in Canada's NCS over time compares to the changes in the United Kingdom's NCS over time) [22].

4. Results

Four core themes emerged from our analysis, which correspond with the second-round codes noted in the previous section: understanding the current environment; teamwork; preparing for the future; and security and protective actions. In some cases, these themes highlighted issues of stability in an NCS over time, while in other cases, the themes pointed to key changes. We describe each theme below, then outline the applicability of the theme to each country.

4.1. Understanding the current environment

A key component of an NCS is to introduce the reader to the concept of cybersecurity and why it is important to a country. As society becomes more connected, adopting cybersecurity practices becomes paramount to mitigating cybersecurity gaps and protecting digital information. Our results indicate that NCS documents typically recognize how cybersecurity can address the challenges of the current digital environment. Moreover, the NCS documents provide examples of cyber threats conducted by cyber threat actors if cybersecurity measures are not adopted.

4.1.1. Canada Both NCS documents recognize the benefits and costs of relying on digital technology. For example, in the 2010 NCS, Canadians are said to be "…embracing the many advantages that cyberspace offers, and our economy and quality of life are the better for it. But our increasing reliance on cyber technologies makes us more vulnerable to those who attack our digital infrastructure to undermine our national security, economic prosperity, and way of life" [23, p. 1]. To highlight the importance of cybersecurity, both NCS documents provide examples of cyber threats (e.g., privacy loss, financial extortion) that illustrate how individuals and/or businesses can be targeted.

4.1.2. The United Kingdom All three versions of the United Kingdom's NCS recognize that embracing the digital environment increases exposure to cyber threats. For instance, the United Kingdom's NCS suggests that the "…use of cyberspace is [characterized] by increasing levels of reliance as government, business, and individuals, continue to benefit from the significant advantages of our increasingly networked society. With this growing dependence, however, comes an increased level of exposure and vulnerability to some of the national security threats that interact with and through cyber space" [24, p. 12]. This NCS also provides examples of cyber threat actors (e.g., criminals, states, terrorists) and methods of attack (e.g., electronic attacks, subversion of the supply chain and radio signals) [24]. Interestingly, we noted that the 2009 NCS introduces cybersecurity in an approachable manner through a question-and-answer format. Questions include "Who is this for? What is cyber space? Why is cyber space important? What do we mean by cyber security? Why does the UK need a cyber security strategy?" [24, pp. 7-9].

4.1.3. Australia All three versions of Australia's NCS recognize the benefits and costs of relying on the current digital environment. For example, the 2020 NCS suggests that "Australians are rightfully seizing the opportunities of our digital world. However, as the opportunities have increased, so too have cyber threats" [25, p. 6]. Further examples of cyber threat actors and cyber consequences are also included to highlight the importance of cybersecurity, such as the following quote from the 2016 NCS: "Australian organizations across the public and private sectors have been compromised by state-sponsored or non-state actors" [26, p. 6].

4.2. Teamwork

Cyber threats can come from anywhere in the world and each individual, business, and government can be targeted. In response, countries have developed comprehensive NCS documents to help mitigate this risk. However, implementing an NCS is a complex task that requires the collaboration and support from multiple stakeholders. Our results indicate that NCS documents highlight the importance of establishing and fostering relationships with domestic (i.e., private sector, academia, local government) and international partners. Moreover, we noted that implementing any one NCS is a collective responsibility in which many stakeholders have a role to play.

4.2.1. Canada Both Canadian NCS documents recognize teamwork as a key component of its strategy and each NCS has a dedicated section focused on teamwork. For example, "Partnering to secure vital cyber systems outside the government" is discussed in the 2010 NCS [23, p. 7], and "Leadership and Collaboration" is discussed in the 2018 NCS [27, p. 31]. Both NCS documents also recognize that cybersecurity is a collective responsibility. For example, the 2010 NCS states that "we all have a role to play as we take full advantage of cyberspace to build a safe, resilient and

innovative Canada" [23, p. 7]. Interestingly, developing the 2018 NCS was also a collective effort. The federal government administered an online public consultation that sought the views of Canadians from the private sector, academia, and other groups on the country's cyber security landscape [27].

4.2.2. The United Kingdom Teamwork is also a prominent theme in the United Kingdom's NCS. For example, the 2009 NCS "…highlights the need for Government, organizations across all sectors, international partners and the public to work together to meet our strategic objectives of reducing risk and exploiting opportunities" [24, p. 8]. Moreover, each version of the NCS recognizes that cybersecurity is a collective responsibility. The 2011 NCS states that "achieving this vision will require everybody, the private sector, individuals and governments to work together. Just as we all benefit from the use of cyberspace, so we all have a responsibility to protect it" [28, p. 22].

4.2.3. Australia The Australian NCS documents discuss teamwork from an international perspective. In the 2009 NCS, Australia notes an intention to actively engage in the international community with countries that have similar concerns about cybersecurity. The international community includes the "United Nations, International telecommunication union (ITU), Asia Pacific Economic Cooperation (APEC) and the Organisation for Economic Co-operation and Development (OeCD)" [29, p. 15]. Moreover, the Australian NCS documents recognize that the success of their implementation depends on the input of ordinary individuals. For example, "not all cyber security risks can be addressed by governments and industry – individuals should also take steps to protect themselves" [25, p. 10]. Finally, similar to Canada, "the Australian government released a public discussion paper to give every Australian a say in the development" of the 2020 NCS [25, p. 17].

4.3. Preparing for the future

The digital environment is constantly changing as new technologies are developed. These advancements can introduce new cyber risks that circumvent existing cybersecurity controls. To avoid being complacent, countries can develop an NCS that addresses the challenges of today, as well as those of the future. Our results suggest that countries prepare for the future digital environment through three methods: investing in research and development, developing the workforce of the future, and supporting the cybersecurity industry for economic growth.

4.3.1. Canada *Research and development* – Compared to the 2010 NCS, the 2018 NCS emphasized research and development to a much greater extent. For example, the 2018 NCS acknowledges that the federal government "… has a role to play to support advanced research" and build expertise in emerging technologies [27, p. 20]. Similarly, the 2018 NCS states that "the Government will focus on emerging areas of Canadian excellence such as quantum computing and blockchain technologies" [27, p. 24]. The 2018 NCS also focuses on partnering with post-secondary institutions. For example, "…there are also great ideas and strong leadership in our schools and our post-secondary institutions that will be instrumental in shaping the future of cyber security in Canada" [27, p. 29].

Workforce of the future – Developing the workforce of the future is not discussed substantively in the 2010 NCS. However, the 2018 NCS recognizes the risk of an ill-equipped workforce. For example, "a shortage of cyber security talent makes it difficult for organizations – including the federal government – to attract and retain the people they need to improve their cyber security or to disrupt cyber threats" [27, p. 10]. Moreover, providing educational and professional opportunities to young adults can increase the baseline of the workforce's cyber literacy. The federal government "…can encourage more students to move into science, technology, engineering, and mathematics (STEM) fields. We can encourage graduates of both STEM programs and other disciplines to specialize in the skills needed for cyber security jobs" [27, p. 22].

Economic growth – Both Canadian NCS documents recognize the importance of developing the cybersecurity industry for economic growth. For example, in the 2010 NCS, cybersecurity is important for "…building a secure and trusted business environment, [that] will foster the productivity and innovation and that drive our economic prosperity" [23, p. 11]. Further, developing and introducing innovative cybersecurity products to the market is a key driver of economic growth. For example, the 2010 NCS states that "we will explore initiatives to ensure that Canadian companies can bring their products to a global market" [23, p. 24].

4.3.2. The United Kingdom *Research and development* – Since the United Kingdom's first NCS, it has continuously expanded the importance of research and development. For example, in the 2011 NCS, the United Kingdom plans to "strengthen [its] academic base by developing a coherent cross-sector research agenda on cyber…" [28, p. 29]. Moreover, the 2016 NCS discusses plans to "commercialize innovation in academia, providing training and mentoring to academics", "establish innovation centers to drive the development

of cutting-edge cyber products", and "provide funding and support for the Academic Centres of Excellence, Research Institutes and Centres for Doctoral Training" [30, pp. 58-59].

Workforce of the future – The United Kingdom has consistently recognized the importance of developing its workforce with the necessary skills and knowledge. For example, the 2009 NCS plans to "ensure the growth of skills and expertise needed by the Government and industry in the cyber security field" [24, p. 23]. The 2016 NCS also recognizes "the lack of young people entering the profession [and] the shortage of current cyber security specialists" [30, p. 55]. To mitigate this risk, "the Government's ambition is to ensure the sustained supply of the best possible home-grown talent…" [30, p. 55].

Economic growth – The United Kingdom's NCS documents recognized the importance of fostering a safe online marketplace to conduct e-commerce and to develop innovative products for the market. For example, the 2016 NCS states that "the Government will support the creation of a growing, innovative and thriving cyber security sector in the UK…" [30, p. 57].

4.3.3. Australia *Research and development* – From its first NCS, Australia has recognized the importance of investing in research and development. For example, in the 2009 NCS, the government will provide "targeted funding and support for cyber security research and development activities" [29, p. 32].

Workforce of the future – Australia's first NCS also discusses the importance of developing its future workforce and expands on this theme in its successive NCS documents. For example, in the 2016 NCS, it states that "[improving] cyber security education at all levels of the education system" and encouraging students to enroll in STEM programs will improve the workforce's baseline cyber literacy [26, p. 55].

Economic growth – Developing the cybersecurity industry for economic growth is also a prominent theme across Australia's NCS documents. For example, in the 2016 NCS, it states that "the Government's commitment to cyber security will help businesses to diversify and develop new markets, laying the foundations for a prosperous future. [Moreover], the Government will also support Australia's cyber security sector to expand and promote their capabilities to the global market" [26, p. 10].

4.4. Security and protective actions

A key component of an NCS is how a country's citizens, critical infrastructure, and digital information will be protected. Our results indicate that NCS documents focus on five areas: identifying cybersecurity gaps, rights and freedoms, standards and guidance, protecting citizens and critical infrastructure, and law enforcement.

4.4.1. Canada *Identifying cybersecurity gaps* – The 2018 NCS focuses on developing the baseline cybersecurity maturity for small and medium-sized enterprises (SMEs). For example, "small and medium enterprises face similar challenges securing their systems and networks as their much larger counterparts but must do so with less expertise and fewer resources. Governments can help correct this asymmetry by providing advice and guidance and enhancing access to cyber security information and tools" [27, p. 20]. To mitigate this risk, the Canadian government launched CyberSecure Canada, a cybersecurity certification program to help small and medium-sized enterprises to defend themselves from cyber threats and to protect their business, clients, and partners.

Rights and freedoms – Compared to the 2010 NCS, the 2018 NCS has a greater emphasis on the importance of protecting the online rights and freedoms. In the 2018 NCS, the federal government states that it will "work with its international partners to advance Canadian interests. This includes advocating for an open, free, and secure internet" [27, p. 32].

Standards and guidance – Similarly, the 2010 NCS does not discuss this theme at length. However, the 2018 NCS does recognize that "organizations have asked for cyber security standards or legislation in Canada to clarify requirements and expectations to improve their cyber security" [27, p. 11].

Protecting citizens and critical infrastructure – This theme has been prominent across both Canadian NCS documents. The 2018 NCS states that "we must and will strengthen the Government's capability to detect, deter and defend against cyber attacks while deploying cyber technology to advance Canada's economic and national security interests" [27, p. 9].

Law enforcement – Both NCS documents discuss the importance of helping law enforcement expand the scope of its policing to the digital environment. For example, the 2010 NCS recognizes that "Canada's law enforcement agencies cannot combat transnational cybercrimes with outdated investigative power and tools" [23, p. 13]. In response, the federal government "improved the capacity of the [Royal Canadian Mounted Police] and law enforcement agencies to combat cybercrime, including initial investments in cybercrime intelligence, investigations and training" [27, p. 6].

4.4.2. The United Kingdom *Identifying cybersecurity gaps* – In the 2016 NCS, the United Kingdom identifies several unique avenues to improve its cybersecurity

capabilities. First, the United Kingdom plans to improve the security within products and ensure that "future online products and services coming into use are 'secure by default'" [30, p. 35]. Second, the 2016 NCS discusses how "current incident management remains somewhat fragmented across government departments… The [National Cyber Security Centre] will deliver a streamlined and effective government-led incident response function…" [30, p. 44].

Rights and freedoms – Protecting online rights and freedoms has been a key attribute of the United Kingdom's NCS. For example, in the 2009 NCS, it states that "we are determined to tackle the threats, but in a way which balances security with respect for privacy and fundamental rights" [24, p. 4]. Moreover, one of the four major objectives of the United Kingdom's NCS is stated in the third objective as "Helping to shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies" [28, p . 40].

Standards and guidance – The United Kingdom's NCS emphasizes development of standards and guidance to establish norms and acceptable behavior. For example, in the 2016 NCS, the government plans to "set the domestic and international framework to protect our interest" and "set standards we expect key companies and organizations to meet" [30, p. 26].

Protecting citizens and critical infrastructure – The United Kingdom's 2016 NCS discusses at length the importance of building capabilities and deterring cyber threat actors to protect its citizens and critical infrastructure. For example, two of the three sections in the implementation plan are DEFEND and DETER. Moreover, the 2016 NCS states that "the UK makes clear that the full spectrum of our capabilities will be used to deter adversaries and to deny them opportunities to attack us" [30, p. 47].

Law enforcement – Since 2009, law enforcement has been an important part of the NCS. For example, "… an effective response to e-crime requires a broad cross-governmental response involving law enforcement, regulators and national security agencies" [24, p. 24]. Moreover, it is important to "enhance the UK's law enforcement capabilities and skills at [the] national, regional, and local level to identify, pursue, prosecute and deter cyber criminals within the UK and overseas" [30, p. 48].

4.4.3. Australia *Identifying cybersecurity gaps* – The 2020 NCS identifies incident management and security by design as important cybersecurity risks to address. Moreover, the 2020 NCS states that "the Australian Government will work with large businesses and services providers to provide SMEs with cyber security information and tools as part of 'bundles' of secure services" [25, p. 10].

Rights and freedoms – Protecting online rights and freedoms has been recognized since Australia's first NCS. For example, in the 2009 NCS it states, "Australia must pursue cyber security policies that enhance individual and collective security while preserving Australians' right to privacy and other fundamental values and freedoms" [29, p. 6]. Surprisingly, we observed a decrease in the emphasis of this theme in Australia's third NCS compared to its first and second.

Standards and guidance – Developing and embracing best practices is a common theme across all NCS versions. For example, in the 2016 NCS, "Australia supports a cyberspace in which states abide by international law and their behaviour is supported and reinforced by agreed norms – or standards for appropriate conduct" [26, p. 9].

Protecting citizens and critical infrastructure – Since the first NCS, "the aim of the Australian government's cyber security policy is the maintenance of a secure, resilient, and trusted electronic operating environment that supports Australia's national security" [29, p. 12]. Similar sentiments are expressed in the second and third versions of the NCS as well.

Law enforcement – Building law enforcement capabilities is a focus in each NCS. For example, in the 2020 NCS it states that, "law enforcement agencies will be given greater ability to protect Australians online, just as they do in the physical world, and will target criminal activity on the dark web" [25, p. 9].

5. Discussion

The existing research literature has largely focused on conducting cross-sectional, point-in-time comparisons of NCS documents between countries. However, comparability may be limited if studies evaluate a country's first NCS version to another country's second or third NCS iteration. Over time, revised versions of an NCS may be more comprehensive than earlier versions and make improvements to address gaps. For example, Schallbruch and Skierka [16] find Germany's revised NCS to be more comprehensive than its first.

Our longitudinal study expands this line of research by examining the changes over time across three additional countries. Similarly, our results indicate that each successive NCS version is more comprehensive since more stakeholders are involved in its development, more details about its action plans are provided, and greater emphasis is placed on certain themes that lacked attention in previous versions. Although it was beyond the scope of this study to determine the underlying drivers of NCS changes, our

study takes a first step towards such an inquiry by recognizing the types of changes that occur. We acknowledge the potential value of comparing the benefits received through incremental improvements to an NCS, versus improvements that are induced by specific problems in a prior NCS version.

Based on the results of our within-country analysis, some themes received more attention as the country developed a more mature NCS. For example, investing in research and development, as well as developing the future workforce (both contained within the "preparing for the future theme") became more important in recent NCS documents as countries recognized the need to prepare the country for a rapidly changing digital environment. On the other hand, we observed that certain themes remained stable across multiple NCS versions. For example, the 'understanding the current environment' and 'teamwork' themes were fairly stable across NCS versions in our sample. In the following section, we discuss the insights that emerged from our cross-country analysis.

5.1. Cross-country NCS patterns

5.1.1. Understanding the current environment

Based on our observations, each NCS consistently recognizes that society heavily relies on the network-based technologies and this trend will likely continue. Although society has benefited from the Internet, each NCS recognizes that this reliance has put our digital information in a vulnerable position. Our results indicated that this theme was commonly acknowledged at the beginning of the NCS and in a personal statement from a member of the ruling political party. For example, in the Canadian 2010 NCS, the Minister of Public Safety states that "our increasing reliance on cyber technologies makes us more vulnerable…" [23, p. 1]. Similarly, the beginning of each NCS introduces the concept of cybersecurity, why it is important, and examples of cyber threat and cyber threat actors.

Overall, our findings suggest that these themes help the NCS articulate the importance of cybersecurity and why the federal government has taken a formal stance on this issue. Providing real-world examples of cyber threats and cyber threat actors helps the reader relate and understand cybersecurity concepts. Overall, this theme is important because it introduces fundamental cybersecurity concepts to the reader, and it highlights the importance of adopting appropriate cybersecurity practices. Overall, this leads to our first proposition:

Proposition 1 *– Each successive NCS version for a country will remain consistent in its emphasis on the current digital environment and provide examples of emerging cyber threats and cyber threat actors.*

5.1.2. Teamwork

Based on our observations, each country's NCS consistently recognizes the importance of collaboration between the federal government and its domestic and international partners. Moreover, each NCS consistently emphasizes how cybersecurity is a collective responsibility that involves individuals, businesses, and governments.

Broadly, this suggests that countries recognize that teamwork is an important theme for an NCS to address. First, the federal government can seek the advice and expertise from its partners to understand emerging technologies and their risks. Second, cybersecurity is a multi-dimensional challenge that affects multiple stakeholders in different ways. For example, individuals may be more concerned with their personal privacy, whereas governments are more concerned about protecting its critical infrastructure and national security. Collaborating with partners can provide important insights to help develop a comprehensive NCS that addresses the unique needs of each stakeholder group. Third, cyber threats are not bounded by traditional borders and cyber threat actors can launch attacks from anywhere in the world. Establishing relationships and shared cybersecurity goals with international partners can mitigate this risk. Fourth, ordinary individuals are ultimately targeted by cyber threats on a day-to-day basis. Individuals need to learn and adopt cybersecurity practices to protect themselves, their families, and their businesses. An NCS cannot be implemented effectively if individuals are not cyber-literate. This leads to our second proposition:

Proposition 2 *– Each successive NCS version for a country will remain consistent in its emphasis that cybersecurity is a shared responsibility and collaboration between the federal government and its partners is important.*

5.1.3. Preparing for the future

Based on our observations, revised versions of a NCS place more emphasis on research and development and developing the workforce of the future. A future-oriented NCS enables a country to be proactive and prepare for future risks. For example, in Canada's first NCS, we noted there was limited discussion of these two themes. However, Canada's second NCS includes a new section "Cyber Innovation", which discusses these two themes at length and provides more examples of actions that the government plans to implement. Moreover, each NCS recognizes the growing importance of cybersecurity for economic growth. This includes developing a safe and secure online environment for individuals and business to conduct e-commerce and supporting companies to introduce new and innovative

cybersecurity products to the marketplace. Therefore, we suggest the following proposition:

Proposition 3 *– Each successive NCS version for a country will increasingly focus on research and development opportunities and workforce development.*

5.1.4. Security and protective actions

Based on our observations, there are interesting similarities and differences across countries. First, each NCS consistently discusses the security and protection of its citizens and critical infrastructure. This finding aligns with our expectations that it is one of the key reasons for an NCS to be developed in the first place. Second, each NCS consistently emphasizes the importance of investing and enabling law enforcement to police in the digital environment. Third, each NCS consistently recognizes the importance of establishing trust and confidence in the federal government's leadership to protect its citizens and its critical infrastructure. Moreover, it is important that individuals, businesses, and governments trust that the digital environment is safe and secure to conduct their online activities. Fourth, we noted that revised NCS documents placed a greater focus on developing standards and guidance to establish a framework of acceptable online behavior. Fifth, revised NCS documents have identified unique cybersecurity gaps to mitigate. Canada's 2018 NCS has taken a strong position in developing the baseline cybersecurity capabilities of SMEs whereas the United Kingdom and Australia have taken a strong focus in incident management and security-by-design in product development. Overall, we observed that security and protection is a prominent theme throughout each NCS, but the underlying elements tend to fluctuate over time. This leads to our fourth proposition:

Proposition 4 *– Each successive NCS version for a country will remain consistent in its emphasis of how the federal government will secure and protect the digital information of its citizens and critical infrastructure, though the ways of achieving this objective will evolve over time.*

5.2. Contributions

We used content analysis to analyze the NCS documents from Canada, the United Kingdom, and Australia between 2009 and 2020. Our results indicate that there is one set of themes (understanding the current environment, teamwork) that is consistently emphasized in each version of an NCS, as well as another set of themes (preparing for the future, security and protective actions) that is more susceptible to change in revised NCS versions.

From a research perspective, our study makes a unique contribution by moving beyond a cross-sectional view of a country's NCS to consider how the strategies change over time across multiple countries. Our resulting four research propositions synthesize the patterns that we have identified and form a basis for future inquiries into contexts where change or stability play an important role in the ongoing development of governmental policy regarding cybersecurity.

From a practical perspective, our results can aid countries that have not published their first NCS or are planning to issue a revised version, as our study provides insights into the themes that other countries have focused their attention on. Investing in research and development and the workforce of the future have garnered increased attention over time and have become important pillars in recent NCS publications. Moreover, the current environment and teamwork themes are foundational elements for all NCS documents.

5.3. Limitations and future research

As with any study, this work is subject to several limitations that provide opportunities for future investigation. First, our analysis focuses on NCS changes in Canada, the United Kingdom, and Australia, but it is unclear if the conclusions we draw can be generalized to other countries. As such, future research should seek to examine NCS changes in regions not addressed in our analysis, as well as in cases where NCS changes occur more or less frequently than in the countries we examined. Second, our study focused exclusively on NCS documents and did not examine supplemental content. Future research could examine supplemental materials, such as cybersecurity action plans. Finally, our study did not consider the impact of political ideology on the development of the NCS. Because the NCS is developed by the federal government, the sentiment, tone, and strategy itself may be influenced by political ideology. For example, Canada's first NCS was issued in 2010 under the Conservative Party of Canada, and its second NCS was issued in 2018 under the Liberal Party of Canada.

6. Conclusion

We undertook a longitudinal study to examine the stability and changes to the NCS documents of Canada, the United Kingdom, and Australia over time. Our results suggest that revised NCS versions share some key elements, such as a growing emphasis regarding the importance of investing in research and development, as well as developing the workforce of the future.

Moreover, we saw consistent attention paid to understanding the current environment and teamwork across each country's initial and revised NCS releases. Overall, our study provides insights into both stable and changing characteristics of NCS documents over time.

7. References

[1] M. Taddeo, "Is Cybersecurity a Public Good?", Minds and Machines, Springer, Geneva, Switzerland, 2019, pp. 349-354.

[2] E. Haapamäki and J. Sihvonen, "Cybersecurity in Accounting Research", Managerial Auditing Journal, Emerald Publishing, Bingley, UK, 2019, pp. 808-834.

[3] K. P. Newmeyer, "Elements of National Cybersecurity Strategy for Developing Nations", National Cybersecurity Institute Journal, Excelsior College, Albany, NY, 2015, pp. 9-19.

[4] E. Luiijf, K. Besseling, and P. de Graaf, "Nineteen National Cyber Security Strategies", International Journal of Critical Infrastructures, Inderscience Publishers, Geneva, Switzerland, 2013, pp. 3-31.

[5] R. Azmi, W. Tibben, and K. T. Win, "Motives Behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy", presented at the Australasian Conference on Information Systems, Wollongong, 2016.

[6] S. O. Johnsen, "A Comparative Study of the Norwegian Cyber Security Strategy vs Strategies in EU and the US – Emerging Cybersafety Ignored", in *25th European Safety and Reliability Conference, ESREL*, Zurich, Routledge, New York, 2015, pp. 1-8.

[7] J. V. Carvalho, S. Carvalho, and A. Rocha, "European Strategy and Legislation for Cybersecurity: Implications for Portugal", Cluster Computing, Springer, New York, NY, 2020, pp. 1845-1854.

[8] O. Osho and A. D. Onoja, "National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis", International Journal of Cyber Criminology, K. Jaishankar, Ahmedabad, Gujarat, India, 2015, pp. 120-143.

[9] L. Kovács, "National Cybersecurity Strategy Framework", Academic and Applied Research in Military and Public Management Science, Ludovika University Press, Budapest, Hungary, 2019, pp. 65-76.

[10] NIST, "Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity", 2015.

[11] D. K. Mulligan and F. B. Schneider, "Doctrine for Cybersecurity", Daedalus, MIT Press, Cambridge, MA, 2011, pp. 70-92.

[12] K.-S. Min, S.-W. Chai, and M. Han, "An International Comparative Study on Cyber Security Strategy", International Journal of Security and Its Applications, SERC, Weston Creek, Australia, 2015, pp. 13-20.

[13] C. S. Teoh and A. K. Mahmood, "National Cyber Security Strategies for Digital Economy", presented at the International Conference on Research and Innovation in Information Systems (ICRIIS), Langkawi, Malaysia, 2017.

[14] D. Adamsky, "The Israeli Odyssey toward its National Cyber Security Strategy", The Washington Quarterly, Taylor and Francis, Oxfordshire, UK, 2017, pp. 113-127.

[15] L. Y. C. Chang and N. Coppel, "Building Cyber Security Awareness in a Developing Country: Lessons from Myanmar", Computers & Security, Elsevier, Amsterdam, Netherlands, 2020, pp. 1-10.

[16] M. Schallbruch and I. Skierka, *Cybersecurity in Germany* (SpringerBriefs in Cybersecurity), Springer, Geneva, Switzerland, 2018.

[17] M. D. Myers, *Qualitative Research in Business & Management,* Sage Publications, Thousand Oaks, CA, 2009.

[18] M. Q. Patton, *Qualitative Research & Evaluation Methods,* Sage Publications, Thousand Oaks, CA, 2002.

[19] P. J. Curran and D. J. Bauer, "The Disaggregation of Within-Person Effects in Longitudinal Models of Change", Annual Review of Psychology, Palo Alto, CA 2011, pp. 583-619.

[20] D. G. Ancona, P. S. Goodman, B. S. Lawrence, and M. L. Tushman, "Time: A New Research Lens", The Academy of Management Review, Academy of Management, Briarcliff Manor, NY, 2001, pp. 645-663.

[21] M. B. Miles and A. M. Huberman, *Qualitative Data Analysis*, Sage Publications, Thousand Oaks, CA, 1994.

[22] R. K. Yin, *Case Study Research and Applications: Design and Methods*, 6th ed., Sage Publications, London, UK, 2018.

[23] Government of Canada, "Canada's Cyber Security Strategy, for a Stronger and More Prosperous Canada", Ministry of Public Safety, Ottawa, ON, 2010.

[24] Cabinet Office, "Cyber Security Strategy of the United Kingdom, Safety, Security and Resilience in Cyber Space", Office of Public Sector Information, Kew, Richmond, Surrey, UK, 2009.

[25] Australian Government, "Australia's Cyber Security Strategy 2020", Home Affairs, National Circuit, Barton, ACT, Australia, 2020.

[26] Australian Government, "Australia's Cyber Security Strategy, Enabling Innovation, Growth & Prosperity", Department of the Prime Minister and Cabinet, Barton, ACT, Australia, 2016.

[27] Public Safety Canada, "Natrional Cyber Security Strategy, Canada's Vision for Security and Prosperity in the Digital Age", Government of Canada, Ottawa, ON, 2018.

[28] UK Government, "The UK Cyber Security Strategy, Protecting and Promoting the UK in a Digital World", Cabinet Office, London, UK, 2011.

[29] Australian Government, "Cyber Security Strategy", Attorney General's Department, National Circuit, Barton, ACT, Australia, 2009.

[30] HM Government, "National Cyber Security Strategy 2016-2021", Cabinet Office, London, UK, 2016.